8M

УДК 681.2

О.В. Мелех, Е.П. Максимович, В.К. Фисенко
Объединенный институт проблем информатики
Национальной академии наук Беларуси, г. Минск
meleh@newman.bas-net.by

Классификация критически важных объектов информатизации по требованиям физической защиты с использованием методов кластерного анализа

Обоснован и реализован подход к классификации объектов информатизации критически важных объектов по требованиям физической защиты с использованием методов кластерного анализа. Сформулированы содержательная и математическая постановки задачи и разработана методика классификации, в основу которой положена идея разбиения множества объектов на непересекающиеся подмножества. Разбиение производится с использованием функции близости и критериев разбиения не по одному, а по множеству показателей и их значений таким образом, чтобы в пределах одной группы требования к физической защите оставались неизменными.

Введение

Под объектом информатизации (ОИ) критически важного объекта (КВО) понимаются средства вычислительной техники (автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные вычислительные машины, а также копировально-множительные средства, в которых для обработки информации применяются числовые методы) вместе с программным обеспечением, которое используется для обработки информации, входит в состав критически важного объекта, используются для обеспечения надежного функционирования и управления процессами объекта, нарушение или прекращение функционирования которого приводит к значительным негативным последствиям для национальной безопасности, международных отношений, экономическому ущербу, ущербу здоровью людей, имуществу и др.

Обеспечение надежного функционирования ОИ КВО достигается реализацией на объекте комплекса средств и систем информационной безопасности (для обеспечения целостности, конфиденциальности и доступности) и его физической защиты от несанкционированного доступа.

Не существует реально двух ОИ, которые бы обладали одинаковыми свойствами информационной безопасности и физической защиты. Различие определяется степенью ценности обрабатываемой информации, ее конфиденциальностью, штатным численным составом пользователей, применением средств физической защиты и т.д. Важную роль при этом играют назначение и характеристики КВО. Однако некоторые ОИ КВО обладают близкими по некоторым критериям свойствами или сходными признаками. Это позволяет провести разбиение всего множества ОИ на непересекающиеся группы и разработать для каждой группы типовые требования безопасности. Типо-

вые требования будут выступать в качестве основы для формирования требований информационной безопасности и физической защиты к конкретной реализации ОИ.

Необходимо при этом учитывать и то обстоятельство, что каждый ОИ является составной частью конкретного КВО, от назначения и государственной принадлежности которого в значительной степени определяется назначение, процесс функционирования, а в конечном итоге и возможный ущерб от реализации угроз информационной безопасности и физической защиты ОИ. Из этого следует, что разбиение ОИ на непересекающиеся группы возможно будет целесообразно проводить для КВО, принадлежащих конкретному ведомству, министерству, государственному органу, финансовому органу и т.д. Этим самым мы ограничим число типовых ОИ, обладающих сходными свойствами, конкретизируем используемые при проведении классификации показатели и более обоснованно затем сформулируем требования информационной безопасности и физической защиты. Конечно, нельзя исключать и другие подходы.

Наконец, считаем целесообразным конкретизировать объект и задачи исследования. Выше речь шла о комбинации видов защиты ОИ: защита информации, обрабатываемой на ОИ, или в более общем виде – обеспечение информационной безопасности и физическая защита ОИ от несанкционированного доступа к нему. Таким образом, в первом случае объектом защиты является информация, а в качестве задачи защиты выступает информационная безопасность, а во втором случае объектом защиты выступает ОИ КВО, а в качестве задачи защиты – физическая защита ОИ от несанкционированного доступа. Задача классификации ОИ по требованиям информационной безопасности рассматривалась в ряде работ, изданы специальные законы и положения по данному направлению [1-3]. Задача классификации ОИ по требованиям физической защиты пока не нашла методической и практической реализации.

Целью настоящей работы является выработка и изложение некоторых возможных и, на наш взгляд, пригодных для практики подходов к классификации ОИ КВО по требованиям физической защиты от несанкционированного доступа.

Для достижения указанной цели необходимо было решить следующие задачи:

– определение цели классификации;

– определение показателей физической защиты ОИ КВО;

– разработка содержательной и математической постановки задачи классификации ОИ КВО по требованиям физической защиты;

– разработка методики классификации ОИ КВО по требованиям физической защиты;

– разработка алгоритма последовательной классификации ОИ КВО по требованиям физической защиты.

Ниже приведены наши предложения по порядку и методам решения указанных задач.

1 Цели классификации объектов информатизации критически важных объектов по требованиям физической защиты

В настоящее время обострилась проблема обеспечения физической защиты как непосредственно КВО, так и главной его информационно-технологической составляющей – объекта информатизации, ввиду обострения таких явлений, как несанкционированный доступ к ОИ, хищение электронных носителей информации, вредительство и терроризм. К сожалению, на настоящем этапе создания КВО и их информационного

обеспечения недостаточно внимания уделяется как введению в действие современных нормативных документов, так и развитию современной методологической и технической базы в области физической защиты ОИ КВО.

Непременным условием нормального функционирования с позиции физической защиты ОИ КВО является своевременное пресечение возможных акций нарушителей. Основными этапами действий потенциального нарушителя при проникновении на объект защиты являются: выявление ОИ, наблюдение за ОИ, разработка вариантов несанкционированного проникновения, реализация основного или альтернативного варианта несанкционированного доступа, уход из ОИ с возможной полной или частичной маскировкой или ликвидацией следов несанкционированного доступа [4]. Поэтому главная цель физической защиты ОИ может быть декомпозирована на такие частные цели, как:

– предотвращение несанкционированного доступа на территорию ОИ и контролируемую зону объекта;

– обнаружение проникшего на ОИ нарушителя до момента, когда он может совершить акцию, и доведение информации о несанкционированном доступе до органов физической защиты;

– своевременное пресечение акции (захват или нейтрализация нарушителя, угрожающего функционированию ОИ), которую может совершить нарушитель, проникший на ОИ;

– принятие всех возможных мер по минимизации ущерба от реализации угрозы ОИ.

Реализация перечисленных подцелей физической защиты ОИ не может осуществиться без внедрения на ОИ современных высокоэффективных способов, систем и средств физической защиты ОИ. Требуемая эффективность указанных способов, систем и средств физической защиты может быть достигнута лишь при соответствии определенным комплексным функциональным и гарантийным требованиям, как это реализуется в области информационной безопасности ОИ [5]. Такие требования не могут быть разработаны ко всему множеству ОИ КВО, принадлежащих различным министерствам и ведомствам. Представляется целесообразным все множество ОИ КВО разбить с использованием специальных критериев принятия решений на типовые классы ОИ, в пределах которых свойства ОИ будут близки по определенным характеристикам, что позволит обоснованно сформулировать требования по физической защите ОИ.

Таким образом, целью классификации ОИ КВО по требованиям физической защиты является проведение классификации ОИ КВО и на этой основе разработка для классов ОИ типовых требований физической защиты на основе интегрального описания свойств ОИ каждого класса. Тогда для того чтобы обоснованно предъявить требования по физической защите к конкретному ОИ, надо или спрогнозировать с позиции физической защиты его будущий облик, если ОИ подлежит созданию, или идентифицировать облик уже действующего ОИ, т.е. определить принадлежность к определенному классу и воспользоваться типовым набором требований, соответствующих данному классу.

2 Содержательная и математическая постановки задачи классификации объектов информатизации критически важных объектов по требованиям физической защиты

Содержательное описание задачи разбиения ОИ КВО на классы типовых представляется следующим образом.

Имеется множество объектов информатизации. Каждый объект характеризуется определенной совокупностью показателей безопасности. Известны результаты измерений каждого показателя и определены параметры (вектора) измерений.

Сущность разбиения объектов информатизации на классы однотипных с точки зрения физической защиты заключается в разбиении множества объектов на непересекающиеся подмножества. Решение этой задачи осуществляется в два этапа.

На первом этапе определяется множество показателей и их параметров (признаковое пространство). Если множество значений каждого из показателей разбить по определенным правилам на непересекающиеся группы, то по каждому показателю могут быть выделены области его значений, в пределах которых требования к физической защите являются неизменными. Однако этого недостаточно. Для различных типовых ОИ разбиение проводится не по одному, а по множеству показателей. Причем каждый показатель определяется множеством значений. Оценка значения показателя характеризует вклад в формирование требований по физической защите ОИ. Следовательно, разбиение множества ОИ на непересекающиеся группы производится не по одному, а по множеству показателей и их значений таким образом, чтобы в пределах одной группы требования к физической защите оставались неизменными.

На втором этапе определяется функция близости и критерий разбиения на множестве ОИ с использованием множества показателей и их значений и формируется заданное число классов типовых ОИ.

Данная задача может быть решена посредством методов кластерного анализа [6]. Кластерный анализ представляет собой совокупность методов для формирования однородных классов в произвольной области больших объемов данных. Они применяются для неформализуемых или плохо формализуемых задач различной физической природы, не использующих априорные предположения о вероятностной природе исходной информации, а использующих эвристические соображения о свойствах объекта. Исходные данные разделяются на кластеры, элементы которых имеют подобные признаки, а для их отличия вводится некоторая целевая функция. В самом общем виде задача кластерного анализа формулируется следующим образом [6]:

Задано множество $\boldsymbol{I = \{I_1, I_2,\ldots,I_n\}}$ объектов, принадлежащих некоторому сообществу. Существует некоторое множество $\boldsymbol{C = (C_1, C_2,\ldots,C_n)}$ характеристик, которыми обладает каждый объект из $\boldsymbol{I}$. Известны результаты измерения характеристик каждого объекта и множество векторов измерений $\boldsymbol{X = \{X_1, X_2,\ldots,X_n\}}$, которые описывают множество $\boldsymbol{I}$.

Требуется на основе данных, содержащихся в множестве $\boldsymbol{X}$, разбить множество объектов $\boldsymbol{I}$ на $\boldsymbol{m}$ кластеров (подмножеств) так, чтобы каждый объект $\boldsymbol{I_i}$ принадлежал только одному множеству разбиения, объекты одного кластера были однородными, а объекты разных кластеров – разнородными.

Математическая постановка задачи может быть **сформулирована** следующим образом.

Имеется множество $\boldsymbol{O}$ ОИ КВО, которые необходимо разбить на классы с тем, чтобы предъявить типовые для каждого класса требования к системе физической защиты. Заранее число объектов не определено. Однако известно, что каждый из объектов множества $\boldsymbol{O}$ определяется множеством $\boldsymbol{P = \{P_1, P_2,\ldots, P_m\}}$ внешнесистемных признаков, которые будем называть показателями разбиения объектов информатизации. Каждый показатель из множества $\boldsymbol{P}$ определяется множеством параметров (значений показателя):

$$P_1 = \{p_{11}, p_{12},..., p_{1j_1}\}, P_2 = \{p_{21}, p_{22},..., p_{2j_2}\}, \ldots,$$
$$P_m = \{p_{m1}, p_{m2},..., p_{mj_m}\}, \quad (1)$$

где m – число показателей;

j_i – число параметров i-го показателя.

Перечень показателей для всех объектов информатизации является одинаковым, т.е. m = const. Число параметров для различных показателей может быть различным.

Параметры показателей могут быть как количественными, так и качественными. Для **i**-го показателя результат оценки (измерения) **j**-го параметра будем обозначать символом $\mathbf{p_{ij}}$.

Для оценок параметров выполняются следующие условия:

$$(p_{11}>p_{12}>\ldots>p_{1j1}),\ (p_{21}>p_{22}>\ldots>p_{2j2}),\ \ldots,$$
$$(p_{m1}>p_{m2}>\ldots>p_{mjm}). \qquad (2)$$

Каждый $\boldsymbol{O_r}$ объект информатизации определяется совокупностью $\boldsymbol{p_{ij}}$ параметров (по одному параметру от каждого показателя), а именно:

$$O_r = \{p_{1r_1}, p_{2r_2}, \ldots, p_{mr_m}\}, \qquad (3)$$

где $r = \overline{1, n}$ – порядковый номер объекта;

$r_i = \overline{1, j_i}$, $i = \overline{1, m}$;

$n = \prod_{i=1}^{m} j_i$ – число объектов.

Очевидно, что совокупность оценок параметров отдельного объекта можно рассматривать как координаты точки в признаковом пространстве, а независимое множество совокупностей оценок параметров всех объектов можно представить как $\boldsymbol{n}$ точек в $\boldsymbol{m}$-мерном признаковом пространстве.

Необходимо на основе множества параметров разбить множество объектов информатизации на $\mathbf{N} < \boldsymbol{n}$ подмножеств (классов) так, чтобы отдельный объект принадлежал одному и только одному подмножеству разбиения и чтобы объекты, принадлежащие одному и тому же подмножеству, были (по некоторому критерию) **однородными**, в то время как объекты, принадлежащие разным подмножествам, были **разнородными.**

3 Показатели физической защиты объектов информатизации критически важных объектов

При выборе показателей физической защиты необходимо учитывать цель физической защиты. С одной стороны, физическая защита направлена на обеспечение нормального функционирования ОИ в условиях возможного несанкционированного доступа, т.е. на обеспечение защиты процессов управления КВО, а с другой стороны, физическая защита ОИ является важным элементом непосредственно защиты КВО. Исходя из этого показатели должны отражать как элементы свойств и характеристик ОИ, так и КВО.

По физическому смыслу показатели физической защиты определяются следующими внешнесистемными свойствами как ОИ, так и КВО:

– организационной политикой физической защиты, принятой на ОИ и КВО;

– уровнями физической защиты ОИ и КВО;

– характеристикой внешней среды безопасности ОИ КВО.

В соответствии с указанными свойствами и на основании имеющегося национального и международного опыта [7-9] предлагаются следующие показатели внешнесистемных признаков ОИ (табл. 1).

Таблица 1 – Показатели внешнесистемных признаков ОИ

Показатель	Параметры показателя	Оценка параметров
Организационная структура управления КВО (P_1)	КВО республиканского значения (P_{11})	p_{11}
	КВО областного значения(P_{12})	p_{12}
	КВО районного значения(P_{13})	p_{13}
	КВО местного значения (P_{14})	p_{14}
Ущерб здоровью и жизни людей, обусловленный нарушением физической защиты ОИ КВО (P_2)	Ущерб от повышенной смертности (P_{21})	p_{21}
	Ущерб от потери трудоспособности (P_{22})	p_{22}
	Ущерб от повышенной заболеваемости (P_{23})	p_{23}
Экономический ущерб, обусловленный нарушением физической защиты ОИ КВО (P_3)	Катастрофический (P_{31})	p_{31}
	Высокий (P_{32})	p_{32}
	Умеренный (P_{33})	p_{33}
	Низкий (P_{34})	p_{34}
	Несущественный (P_{35})	p_{35}
Снижение качества выполнения основных процессов ОИ КВО (P_4)	Нарушение основных процессов, срыв задач управления (P_{41})	p_{41}
	Снижение эффективности выполнения процессов, функций (задач) (P_{42})	p_{42}
	Несущественные ошибки в системах или процессах и в управлении (P_{43})	p_{43}
Уровень физической защиты ОИ КВО (P_5)	базовый уровень (P_{51})	p_{51}
	расширенный уровень (P_{52})	p_{52}
	усиленный уровень (P_{53})	p_{53}

Кратко рассмотрим содержательную часть каждого показателя и его параметров.

Организационная структура управления ОИ КВО (P_1)

В качестве организационной структуры управления ОИ КВО предлагается различать ОИ КВО по признаку государственных приоритетов системы национальной безопасности:

– *ОИ КВО республиканского значения* – республиканский уровень административного управления (Совет министров, Совет национальной безопасности и т.д.);

– *ОИ КВО областного значения* – областной уровень административного управления (областные органы управления и власти);

– *ОИ КВО районного значения* – районный уровень административного управления (районные органы управления и власти);

– *ОИ КВО местного значения* – местный уровень административного управления (городские/сельские органы управления и власти).

Потенциальная опасность нарушения физической защиты ОИ КВО определяется важностью информации, которая используется для управления технологическими процессами критически важного объекта. Фактически речь идет о создании чрезвычайной ситуации, обусловленной нарушением управления технологическими процессами.

Под чрезвычайной ситуацией понимается состояние, при котором в результате несанкционированного действия на критически важном объекте нарушаются нормальные условия его работы, возможно нанесение ущерба здоровью персонала (населения),

возникает угроза жизни персонала (населения), а также возможно нанесение ущерба окружающей среде. В соответствии с этим предлагаются следующие показатели ущерба от отказа (нарушения функционирования) ОИ КВО вследствие нарушения физической защиты ОИ КВО.

Ущерб здоровью и жизни людей, обусловленный нарушением физической защиты ОИ КВО (P_2)

– *Ущерб от повышенной смертности.* Гибель людей или многочисленные повреждения с угрозой для жизни.

– *Ущерб от потери трудоспособности*. Повреждения с угрозой для жизни, вызывающие необходимость госпитализации, а также серьезные повреждения, требующие госпитализации или многократного обращения за лечебной помощью.

– *Ущерб от повышенной заболеваемости.* Повреждения или заболевания, не требующие помощи лечебного учреждения.

Экономический ущерб, обусловленный нарушением физической защиты ОИ КВО (P_3)

Экономический ущерб может быть оценен на день инцидента и может быть вычислен как определенный процент (%) от стоимости активов ОИ КВО.

– *Катастрофический.* Экономический ущерб ≥ 15,0%.

– *Высокий.* 10,0% ≤ Экономический ущерб < 15,0%.

– *Умеренный.* 5,0% ≤ Экономический ущерб < 10,0%.

– *Низкий.* 2,5% ≤ Экономический ущерб < 5,0%.

– *Несущественный.* 1,0% ≤ Экономический ущерб < 2,5%.

Снижение качества выполнения основных процессов ОИ КВО (P_4)

– *Нарушение основных процессов, срыв задач управления*. Сектор инфраструктуры может прекратить функционирование. Разрушающее воздействие на сегменты отраслевых инфраструктур страны и зарубежья.

– *Снижение эффективности выполнения процессов, функций (задач).* Невыполнение одного и нескольких ключевых требований управления. Умеренное воздействие на основные процессы (функции) ОИ других объектов.

– *Несущественные ошибки в системах или процессах и в управлении*, требующие корректировок без влияния на общий ход процессов. Отсутствие воздействия на основные процессы других систем.

Уровень физической защиты ОИ КВО (P_5)

При выборе необходимого уровня физической защиты предлагается учитывать возможность обоснованного отнесения ОИ КВО к одной из четырех категорий КВО: 1) особо важный объект; 2) особо режимный объект; 3) режимный объект; 4) нережимный объект.

Выбор уровня физической защиты также во многом зависит от многих конкретных факторов, таких как конфигурация территории, рельеф местности, геомагнитная обстановка, структура расположения жизненно важных центров объекта, характер угроз и многое другое. В зависимости от этого предлагаются следующие уровни защиты.

Базовый уровень физической защиты, при котором защита объекта информатизации осуществляется средствами критически важного объекта.

Расширенный уровень физической защиты, при котором базовый уровень дополняется средствами непосредственной физической защиты от несанкционированного доступа к объекту информатизации.

Усиленный уровень физической защиты, при котором расширенный уровень дополняется специальными средствами, связанными со значимостью объекта информатизации, его потенциальной опасностью и условиями функционирования.

В зависимости от особенностей ОИ КВО и, возможно, цели классификации ОИ КВО правомерно использовать и другие показатели.

Оценка значения параметра показателя физической защиты характеризует вклад в физическую защиту ОИ. Значение оценки может быть определено экспертным путем. Следует заметить, что экспертные методы, при правильно подобранных экспертах, более чем в 90% случаев совпадают с точными численными методами оценки [6]. Оценка значений параметров проводится специалистами в области комплексного обеспечения информационной безопасности, так как от результатов этой оценки будет зависеть не только качество классификации ОИ КВО, но и в последующем, что очень важно, надежность и эффективность общей системы безопасности. Следует учитывать также приоритетность в обеспечении безопасности информации, которая определена организационной политикой безопасности организации. Как правило, всегда существует показатель классификации, который является с позиции безопасности приоритетным, остальные показатели также являются важными, но в меньшей степени, чем основной показатель.

4 Методика классификации объектов информатизации критически важных объектов по требованиям физической защиты

Имеется множество ***O*** ОИ КВО, которые необходимо разбить на заданное количество классов с тем, чтобы предъявить типовые для каждого класса требования к системе физической защиты. Заранее число объектов не определено. Однако известно, что каждый из ОИ КВО множества ***O*** определяется множеством $\boldsymbol{P = \{P_1, P_2\ P_3, P_4, P_5\}}$ показателей разбиения ОИ. В соответствии с (1) каждый показатель из множества ***P*** определяется множеством параметров (значений показателя):

$P_1 = \{p_{11}, p_{12}, p_{13}, p_{14}\}$,

$P_2 = \{p_{21}, p_{22}, p_{23}\}$,

$P_3 = \{p_{31}, p_{32}, p_{33}, p_{34}, p_{35}\}$,

$P_4 = \{p_{41}, p_{42}, p_{43}\}$,

$P_5 = \{p_{51}, p_{52}, p_{53}\}$.

Для оценок параметров выполняются следующие условия (2):

$(p_{11}>p_{12}> p_{13}> p_{14})$,

$(p_{21}>p_{22}> p_{23})$,

$(p_{31}>p_{32}> p_{33}> p_{34}>p_{35})$,

$(p_{41}>p_{42}> p_{43})$,

$(p_{53}>p_{52}> p_{51})$.

Пусть каждый объект характеризуется показателями $P_1,...,P_5$ и соответствующими параметрами $\boldsymbol{p_{11},\ldots, p_{53}}$. Тогда получим следующий перечень объектов и соответствующих параметров:

$$O_1 = F_1(p_{11,} p_{21}, p_{31}, p_{41}, p_{51});\ O_2=F_2(p_{11,} p_{21}, p_{31}, p_{41}, p_{52});\ \ldots;$$

$$O_n = F_n(p_{24,} p_{23}, p_{35}, p_{43}, p_{53}).$$

Получим n = 4×3×5×3×3 = 540 ОИ КВО с заданными оценками параметров, которые подлежат распределению по классам.

Для решения задачи классификации ОИ КВО необходимо количественно определить понятия *однородности* и *разнородности* объектов. Что означает: «два объекта O_i и O_j разнородны или различны?». Задача была бы решена, если бы O_i и O_j объекты попадали в один и тот же класс всякий раз, когда расстояние (отдаленность) между соответствующими точками O_i и O_j было бы «достаточно малым», и наоборот, попадали бы в разные классы, если расстояние между указанными точками было бы «достаточно большим». Таким образом, **в качестве критерия оптимальности разбиения (целевой функции)** объектов по классам может быть **принято расстояние между точками O_i и O_j, что эквивалентно расстоянию между объектами O_i** и O_j.

В [6] приведены некоторые функции расстояния между объектами.

Евклидова метрика очень популярна и наиболее употребительна в практике. Воспользуемся подходом, рекомендуемым в [6].

Евклидово расстояние между объектами O_i и O_j определяется соотношением

$$d_{ij} = \left[\sum_{k=1}^{m} (p_{ki} - p_{kj})^2 \right]^{\frac{1}{2}}, \qquad (4)$$

где m – число показателей классификации.

Оценки в точках $O_1, O_2, ..., O_n$ могут быть представлены в виде матрицы параметров размером m × n:

$$\mathrm{O} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ . & . & \cdots & . \\ p_{m1} & p_{m2} & \cdots & p_{mn} \end{pmatrix} = \left(\mathrm{O}_1, \mathrm{O}_2, ..., \mathrm{O}_n\right). \qquad (5)$$

С использованием (5) можно определить расстояния между каждой парой ОИ КВО, результаты которых могут быть представлены в виде симметричной матрицы расстояний:

$$D = \begin{pmatrix} 0 & d_{12} & ... & d_{1n} \\ d_{21} & 0 & ... & d_{2n} \\ . & . & ... & . \\ d_{n1} & d_{n2} & ... & 0 \end{pmatrix}. \qquad (6)$$

Диагональные элементы матрицы $d_{ii} = 0$ для $i = 1, 2, ..., n$. Матрица (6) является исходной для разбиения объектов по классам.

5 Число классов объектов информатизации

Вопрос о числе классов ОИ КВО является сугубо субъективным. Максимальное число классов равно числу объектов, т.е. каждый объект относится только к одному классу и одному классу принадлежит только один объект. Чем больше число классов, тем точнее могут быть сформулированы требования к физической защите ОИ КВО, исходя из внешнесистемных признаков (показателей) объекта. Однако никогда нельзя быть уверенным в том, что рассматриваемый ОИ КВО действительно обладает такими конкретными признаками, которые присущи данному классу ОИ КВО. Так как заранее трудно предсказать и условия расположения, и условия применения, и число пользователей, и т.д. Поэтому практически при проектировании физической защиты ОИ КВО используют общие требования безопасности, которые формулируются для ти-

повых объектов, входящих в данный класс. Примером таких общих требований являются функциональные и гарантийные требования, которые формулируются в профилях защиты для типовых ОИ [5]. Конкретные требования безопасности формулируются в задании по обеспечению безопасности для рассматриваемой реализации объекта. Исходя из этих соображений, нет необходимости вводить большое число классов.

Возможен и другой крайний случай, когда все возможные варианты ОИ КВО объединяются в один класс – «критически важные объекты информатизации». Естественно, что в этом случае требования к физической защите будут настолько общими, что их практическое использование станет проблематичным.

На наш взгляд, целесообразно введение не более четырех-пяти классов ОИ КВО.

6 Алгоритм последовательной классификации объектов информатизации критически важных объектов по требованиям физической защиты

Схема последовательной классификации ОИ КВО может быть описана так же, как она предложена в [6] применительно к кластеризации.

Для придания большего значения более отдаленным друг от друга объектам в качестве меры расстояния примем квадрат евклидовой метрики (d^2_{ij}). С использованием (4), далее вычисляется матрица $\boldsymbol{D} = \{d^2_{ij}\}$, где d^2_{ij} – квадрат расстояния между объектами O_i и O_j.

Максимальное расстояние получится между O_1 и O_n объектами. Это следует из вышеуказанного предположения, что параметры каждого из показателей, представленные в табл. 1, заранее упорядочены: более жесткие требования к физической защите по каждому показателю определяются параметром с большим значением оценки.

При $i \neq j$ все возможные значения расстояний между объектами лежат в пределах от D_{min} до D_{max}. Величину $D_{min} = min\ d(O_i, O_j)$ будем называть минимальным расстоянием между ОИ КВО, а величину $D_{max} = max\ d(O_i, O_j)$ – максимальным расстоянием между ОИ КВО.

Существуют различные теоретические способы разбиения объектов по классам. В [6] приведен ряд оптимальных способов, которые не только позволяют проводить разбиение объектов по классам, но и оптимально определять число классов.

На практике предлагается использовать более простые способы – так называемые методы одиночной связи и полной связи между объектами [7]. Применительно к рассматриваемой в данной статье задаче указанные методы определяются следующим образом. Предположим, что множество $\boldsymbol{O} = \{O_1, O_2, ..., O_n\}$ ОИ КВО необходимо разбить на $\boldsymbol{N}$ классов. Интервал значений расстояний между объектами от D_{min} до D_{max} методом половинного деления разбиваем на $\boldsymbol{N}$ участков.

Верхние границы участков $D_{\max_N}$ определяются выражением

$$D_{\max_N} = D_{\min} + \frac{D_{\max} - D_{\min}}{2^{(N-1)}}. \qquad (7)$$

Вначале объединяются в один класс два объекта, для которых оценки параметров показателей самые высокие. Очевидно, что расстояние между ними будет равно D_{min}.

После этого можно применить один из вышеуказанных способов формирования классов.

Согласно методу *одиночной связи* класс формируется по правилу: новый объект включается в уже сформированный класс, если расстояние между рассматриваемым новым объектом и хотя бы одним из объектов уже сформированного класса лежит в пределах:

для первого класса: от D_{min} до $D_{\max_N}$;

для второго класса: от D_{min} до $D_{\max_{(N-1)}}$;

для третьего класса: от D_{min} до $D_{\max_{(N-2)}}$ и т.д.

Согласно методу *полной связи* класс формируется по правилу: новый объект включается в уже сформированный класс, если расстояние между рассматриваемым новым объектом и каждым из объектов уже сформированного класса лежит в пределах:

для первого класса: от D_{min} до $D_{\max_N}$;

для второго класса: от D_{min} до $D_{\max_{(N-1)}}$;

для третьего класса: от D_{min} до $D_{\max_{(N-2)}}$ и т.д.

Класс считается сформированным, если ни один из оставшихся ОИ КВО не удовлетворяет вышеуказанным условиям.

Затем рассматривается новая пара ОИ КВО, расстояние между которыми лежит в заданных пределах, и происходит формирование нового класса. Процесс анализа продолжается до тех пор, пока все объекты не будут распределены по группам. Естественно, что для самого низшего класса требования к физической защите будут наименее жесткими. И наоборот, к объектам высших классов предъявляются более жесткие функциональные и гарантийные требования к физической защите.

Заключение

Сформулирована и решена задача классификации объектов информатизации критически важных объектов с позиции физической защиты с использованием методов кластерного анализа. Разработанную методику и алгоритм классификации предполагается использовать при проведении классификации объектов информатизации критически важных объектов, принадлежащих различным государственным органам, в соответствии с Планом первоочередных мероприятий, утвержденным правительством Республики Беларусь.

Литература

1. СТБ 34.101.30-2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация.
2. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992.
3. СТБ П 34.101.38-2009. Информационные технологии и безопасность. Классификация объектов информационных технологий по требованиям информационной безопасности.
4. Белов С.В. Автоматизированная система анализа физической защищенности объектов обработки информации : дис. ... канд. техн. наук / С.В. Белов. – Астрахань, 2005. – 140 с.
5. International Standard. Information technology. – Security techniques. – Evaluation criteria for IT security. – Part 1 : Introduction and general model. – Part 2 : Security functional requirements. – Part 3 : Security assurance requirements. – ISO/IEC 15408 : 1999(E).
6. Дюран Б. Кластерный анализ / Б. Дюран, П. Оделл ; пер. с англ. Е.З. Демиденко ; под ред. А.Я. Боярского. – М. : Статистика, 1977.

7. Кирсанов Ю.Г. Методика категорирования автоматизированных систем по уровню защищенности информации от несанкционированного доступа / Ю.Г. Кирсанов и др. // Вопросы защиты информации. – 1997. – № 3-4. – С. 36-39.
8. Вишняков С.М. Системы комплексной безопасности, категории и уровни защищенности стационарных объектов / С.М. Вишняков // Системы безопасности. – Февраль-март, 2004. – № 1 (55).
9. Зуев А.Г. Категорирование потенциально опасных объектов как основа создания эффективных систем обеспечения безопасности / А.Г. Зуев // Системы безопасности. – Июнь-июль, 2002.
10. Бешелев С.Д. Математико-статистические методы экспертных оценок / С.Д. Бешелев, С.Д. Гурвич. – М. : Статистика, 1980.
11. Анищенко В.В. О некоторых подходах к категорированию объектов информатизации по требованиям информационной безопасности / В.В. Анищенко и др. // Комплексная защита информации. – Минск : Ин-т техн. кибернетики НАН Беларуси, 2000. – С. 5-21.

О.В. Мелех, О.П. Максімовіч, В.К. Фісенко

Класифікація критично важливих об'єктів інформатизації за вимогами фізичного захисту з використанням методів кластерного аналізу

У статті обґрунтований та реалізований підхід до класифікації об'єктів інформатизації, як критично важливих за вимогами фізичного захисту, з використанням засобів кластерного аналізу. Сформульовані змістовна і математична постановки завдання та розроблена методика класифікації, до основи якої покладена ідея розбиття множини об'єктів на підмножини, що не перетинаються. Розбиття виконується з використанням функції близькості і критеріїв, побудованих на множині показників і їх значень так, щоб в межах однієї групи вимоги до фізичного захисту залишалися незмінними.

O.V. Melekh, E.P. Maksimovich, V.K. Fisenko

Classification of Critical Information Objects by the Requirements of Physical Protection Using Methods of Cluster Analysis

The approach to critical information objects classification by physical security requirements on the basis of the cluster analysis is proposed. Informal and mathematical problem statements are formulated. The classification methodology on the basis of objects set partitioning on non-overlapping subsets is developed. The partitioning is performed using adjacency function and partitioning criteria on the basis of set of factors in such manner that physical security requirements are the same within every objects group.

Статья поступила в редакцию 19.07.2010.